InDetail

Bloor

# SolarWinds Log & Event Manager

...a full-functioned, yet affordable, SIEM

An InDetail Paper by Bloor Research
Author : Fran Howarth
Publish date : January 2014

SolarWinds LEM provides all of the essential features required of a SIEM, but at a fraction of the cost of many competing products.

Fran Howarth

# Executive summary

SolarWinds Log & Event Manager (LEM) is a security information and event management (SIEM) system. It is based on technology that it acquired from TriGeo, which released its first SIEM product in January 2002. As such, it is a mature product that has been on the market for as long as most of its competitors.

LEM is primarily aimed at the mid-market, although it is also used by a wide range and number of large enterprises. It provides the core functionality of enterprise-class products offered by competing vendors, including real time centralised event and log collection, correlation, analysis and storage from virtually every system that makes up an organisation's IT infrastructure. SolarWinds also offers extensive remediation capabilities to automate response.

LEM allows organisations of all sizes to meet the security monitoring, incident response and compliance challenges that they face in an efficient yet affordable manner since the product is a fraction of the cost of competing offerings. Many smaller organisations face the same challenges and mandates as their larger counterparts, but lack the budget or resources to invest in and deal with expensive, complex, technology platforms. LEM is also easy to deploy, use and manage for those without specialist security expertise, with its features designed with ease of use as the foremost priority.

This paper describes the core capabilities of SolarWinds LEM, explains the factors that differentiate it from competitors and discusses the use cases in terms of the problems that LEM can help to solve. It is intended as a primer for any organisation that is looking to improve its ability to enhance its overall security posture, respond to security incidents and meet compliance challenges in a cost-effective manner.

## Fast facts

- SolarWinds LEM will aid organisations by helping them to more efficiently manage the security of their IT infrastructure, allowing them to more quickly and easily detect threats, prevent breaches and respond to incidents before damage is done.
- With LEM, organisations will more easily be able to implement security management frameworks that will help to instil trust among business partners and customers in the security management practices of those organisations.
- By implementing LEM, organisations will be better able to achieve compliance with the regulations and industry standards that they face, many of which identify proactive monitoring as a key best practice.

## Key findings

In the opinion of Bloor Research, the following represent the key facts of which prospective users should be aware:

- SolarWinds LEM is a mature technology that has been proven to be effective for companies of all sizes, from the smallest firm to large multinationals.
- Aimed primarily at the mid-market, it is an affordable option, with functionality that rivals that of competing enterprise-class products.
- The direct download model espoused by SolarWinds makes the product easy to acquire and deploy. It is an all-in-one virtual appliance with many out-of-the-box capabilities that drastically reduces the time it takes to be up and running.
- LEM was developed with an emphasis on usability, with tools such as visualisation capabilities and Active Response greatly aiding in the ability to automatically remediate security incidents through integrated threat response capabilities.
- The support offered by SolarWinds is comprehensive and the first year is built into the purchase price.
- SolarWinds is constantly innovating, adding new features and capabilities to LEM in regular updates that are free of charge to customers in perpetuity.
- SolarWinds maintains an active online user community, known as thwack, where users can help drive the product roadmap through feedback and feature requests.

## The bottom line

SolarWinds LEM provides all of the essential features required of a SIEM, but at a fraction of the cost of many competing products. It boosts the capabilities of organisations of any size to improve their overall security posture, detect and remediate security threats, and achieve compliance objectives.

# The product

## Implementation of the product

SolarWinds sells its technology products directly from its website, from which users can download an executable for immediate implementation. It is delivered as an all-in-one virtual appliance that runs on either VMWare or Hyper-V. The operating system and database are packaged into the virtual appliance, with no additional hardware required. Upon download, the user is provided with a wide range of out-of-the-box tools, including setup wizards, charts, graphs and lists, as well as direct access to support documentation that includes both quick start and full user guides. There are also a number of tools to allow users to customise the implementation, such as developing specific correlation rules. Some of the more advanced features require the deployment of additional agents, as does support for systems that do not use SNMP/Syslog.

The first year of unlimited 24/7 phone and email support is included in the product purchase price and further support resources are available online in its comprehensive thwack community that offers forums, additional tools, and the ability to share best practices and request new product features. Thwack is used by some 125,000 people.

## Features

SolarWinds regularly releases upgrades to its LEM product to provide usability and performance enhancements. The latest release is version 5.7. The features that it offers are aimed at providing mid-market customers with the main features of products aimed at large enterprises, but without some of the more sophisticated high-end features that might be required by organisations with specialised security teams or security operations centres. For ease of use, all features are powered using drag-and-drop functionality.

Among the main features available in the SolarWinds LEM offering are:

**Real time event collection and correlation for immediate threat detection**
Logs and event data are captured by the system in real time from a wide variety of data sources from throughout the IT infrastructure, with support for new systems added with each product upgrade. Sources include network devices, security appliances and controls, servers, databases, virtual machines, and cloud systems and applications. All logs and events can be collected in one central location from multiple sites via virtual LEM appliances, even across geographically remote data centres and branch offices. The agents used for collecting data encrypt all records in transit from source to destination for security and chain of custody purposes.

For event correlation, all data collected is processed and analysed before being sent to the database to allow for real time correlation to spot and respond to security threats and vulnerabilities as they occur. There are approximately 700 event correlation rules built into the system out of the box, along with the ability to easily create new rules specific to an organisation as required.

## The product

**Integrated Active Responses for automated remediation**
SolarWinds' LEM provides an extensive library of Active Responses—automated remedial actions to be taken in response to certain security, operational or policy-driven events that are flagged during the data collection and correlation processes. Such responses include actions such as quarantining infected machines, blocking IP addresses, creating, disabling or deleting user accounts, detaching USB devices, logging off users, shutting down machines and sending alerts related to incidents. In addition to the built-in library, the system provides the ability for users to easily create new Active Responses according to their particular needs.

The Active Response mechanisms allow organisations to immediately and automatically remediate all events that are out of line with policy or expected behaviour, such as unauthorised access, unwanted configuration changes or abnormal traffic patterns that could indicate a compromise.

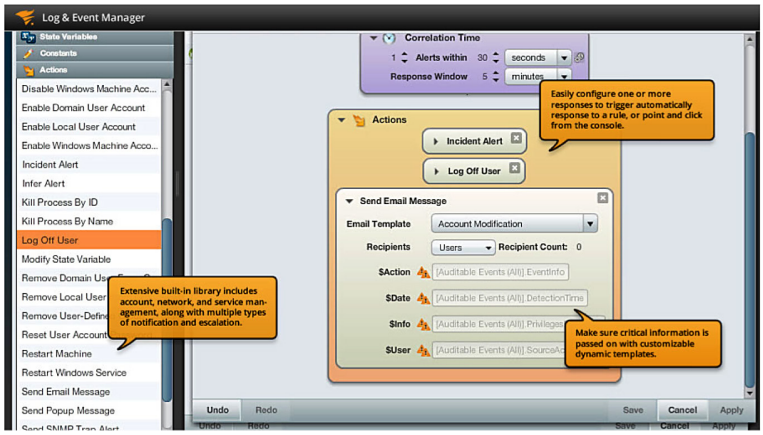


**Figure 1:** Active Responses

**Advanced search and data visualisation for forensic analysis**
An integrated search engine allows all historic events to be analysed forensically from normalised or raw log data, with enhancements in the latest version that allow organisations to schedule searches to run automatically, either once or on a recurring basis. As well as basic keyword searches, drag-and-drop functionality provides the ability to quickly build even complex searches, which can be saved for reuse as required. All search results can be exported to the central management console in a variety of formats.

For ease of use, as well as providing event lists, LEM provides visualisation tools for making the search function more usable. These include word clouds, tree maps, histograms and charts to make it easier and more intuitive to visualise events occurring across the network, both in real time and historically, in order to spot anomalies and trends over time.

## The product

As well as being able to correlate events and remediate events in real time, the LEM system provides long-term storage and archiving of all data collected, with all data highly compressed to reduce the need for extra storage systems to be added. To meet security and data retention requirements, encryption and digital signatures are automatically applied for both archived data and the data stores.

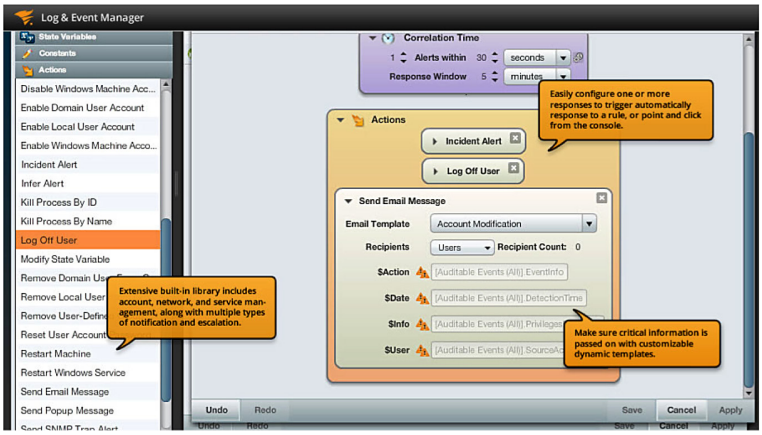


**Figure 2:** Search and forensic analysis

### USB Defender for endpoint data protection

SolarWinds' LEM extends security protections beyond network devices to USB storage systems that users connect to the network. This feature allows organisations to control what devices are able to connect, to monitor what files and applications they are accessing in real time, and to block any actions taken by USB devices that are out of line with policy. In addition, the use of USB devices can be allowed or blocked according to policy or by developing a whitelist of accepted devices. All USB usage is recorded by the system as an audit trail that can be correlated with network logs to detect any malicious activity that has got through defences. The end result is an extra layer of defence to prevent unauthorised USB use and protect against internal data loss.

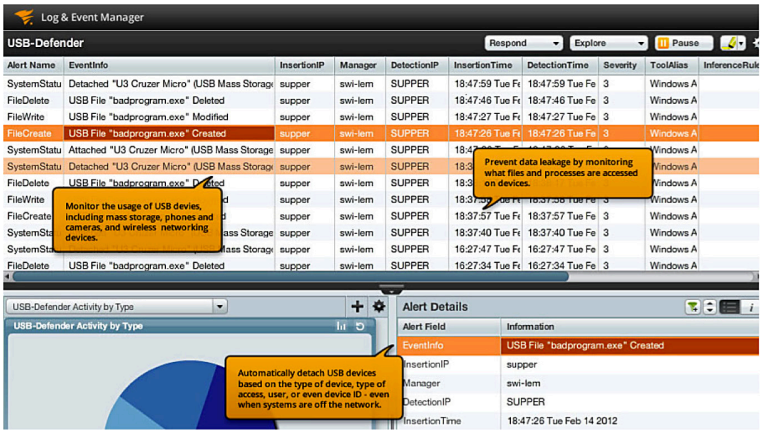


**Figure 3:** USB Defender

## The product

**Workstation and user activity monitoring for internal threat protection**
LEM can monitor all activity occurring on workstations and collect, analyse and store all logs generated. It is intended to aid organisations in their ability to guard against threats and security incidents from internal sources, such as unauthorised users logging onto the network via workstations. Capabilities include the ability to prevent prohibited or unexpected applications from being launched, and to prevent changes from being made to user and group accounts, and to configuration settings.

**Built-in templates for regulatory compliance reporting**
All event logs are stored in a central location, which includes a reporting console for audit and compliance purposes. Provided within this console are pre-packaged report templates designed to meet the requirements of a wide range of international, local and industry-specific regulations and standards, with some 300 templates provided in total. Where a specific template is not available, organisations can easily develop custom forms to cover their needs. This feature makes it easier for organisations to comply with the mandates that they face without the need to implement complex and costly governance, risk and compliance solutions.

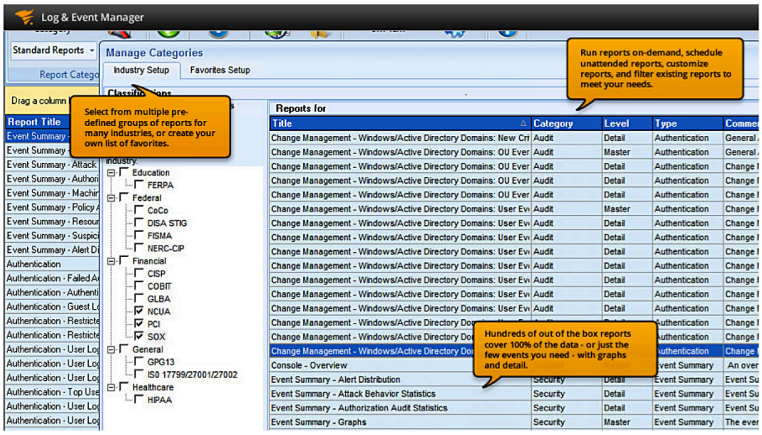


**Figure 4:** Compliance reporting

### Differentiators

The primary differentiators of SolarWinds' LEM product are that it provides an easy-to-use yet comprehensive SIEM and log management solution aimed at the needs of mid-market organisations that often lack the IT and security resources of their larger counterparts, often leaving what resources they do have over-stretched. Such organisations have many of the same needs as larger enterprises—especially with regard to complying with regulations such as data protection and with managing the overall security of their networks. The distribution and implementation model espoused by SolarWinds makes the product easy to evaluate and buy, with a 30-day evaluation period offered for all products, and it is easy to deploy and maintain.

However, LEM is also popular with, and widely used by, a large number of enterprise customers, including more than 425 of the Fortune 500, and is helped by its proven scalability and ability to store massive amounts of data. As well as being deployed across such organisations, it is highly suited to the needs of departments, business units and branches within such organisations.

## The product

A particular differentiator is the value for money that is offered by the LEM product. With LEM, organisations get the core capabilities they need to improve their security posture and help ensure continuous compliance, but at a fraction of the cost of competing solutions. This core functionality includes real time collection, correlation and analysis of log and event data from a wide variety of sources throughout the IT infrastructure, along with the ability to normalise, store, search, and report on log data to help meet security and compliance objectives. On top of this core functionality, LEM offers a set of features that set it apart from its competitors, including in-memory event correlation, built-in automated responses, USB defence technology and data visualisation tools.

Another prime differentiator of SolarWinds' LEM product is its ease of deployment and use. Downloadable from the internet, it can generally be deployed without outside help either from the vendor or from consultants. LEM offers many features that make it extremely easy to use right out of the box without the need for security expertise, including hundreds of built-in rules, filters, searches and reports, with everything governed by a centralised management console with a drag-and-drop interface. Where support is required, 24 x 7 phone and email support is included in the purchase price. Plus, there is a dedicated support site, thwack, which has more than 100,000 IT professional community members. Directly accessible from inside the product, it functions as an online community for sharing and solving problems, tips and tricks, discussing best practices, downloading extra tools, requesting additional features be added to the product, and for sharing custom applications and plug-ins. It provides extensive support documentation and tutorials, and provides information regarding new features and capabilities.

### Supporting products

Recent enhancements and upgrades have seen tighter integration with other products from the IT management tools offered by SolarWinds in its overall product portfolio. These integrations allow for bidirectional information exchange between the products. Among the integrations is that with its Server & Application Monitor (SAM) product for adding visibility into server and application performance, for correlating alerts from SAM with events captured in LEM, and for creating new rules and enhancing correlation notifications for improving incident response capabilities. LEM also integrates with SolarWinds' Alert Central for incident escalation and response to events captured by and forwarded from LEM. Integration with the Network Performance Monitor product allows for network fault, performance and availability monitoring.

# Use cases

### Threat detection and defence

SIEM systems aid organisations in efficiently managing the security of their IT infrastructure. They provide centralised monitoring and management of event and log data generated from hardware systems and applications in use in the organisation—from those directly connected to the network to those connecting remotely. SIEM systems are essential parts of any organisation's security arsenal, allowing them to detect threats, prevent attacks and incidents from occurring, and responding to incidents that do occur.

The need for SIEM systems is growing and will continue to do so. Organisations' networks face more threats than ever before from well resourced and ever more determined attackers with increasingly sophisticated tools at their disposal. Every organisation should consider itself not only a target, but should also assume that it has already been breached. According to the 2013 information security breaches survey undertaken by PwC in association with Infosecurity Europe, 93% of large organisations admitted to suffering at least one security breach in the previous year, as did 87% of small organisations—for that latter, that is up from 76% the previous year. As well as that, organisations that suffered breaches reported experiencing roughly 50% more incidents on average than the previous year. Organisations also have to deal with an ever-wider range and number of users, devices and applications connecting to their networks, making them increasingly harder to police without effective, automated tools.

With the use of SIEM systems, organisations are in a better position, through real time analysis of alerts from throughout the network to see how widely attacks have propagated, to react faster to events that are uncovered and to prioritise remediation efforts where attention is needed the most. SIEM systems provide the situational awareness that is required for actionable intelligence regarding the security threats that they face both in real time and in terms of troubleshooting and forensics of past events to spot trends and bolster defences further.

### Compliance and reporting

As well as helping in managing the security of the IT infrastructure, SIEM systems also have a vital role in helping organisations manage compliance with the regulatory mandates and industry standards that they face. Whilst this burden may be greatest in the public sector or for large enterprises in heavily regulated industries, organisations of all sizes face some level of regulation or must comply with certain industry standards. For example, any organisation that handles payment card information must comply with the requirements of the Payment Card Industry Data Security Standards (PCI DSS) and adherence to information security management frameworks such as those in the ISO 27001 family is growing steadily, especially in Europe and among small firms as well as large.

Data protection legislation is one area where compliance requirements for organisations of all sizes are set to expand rapidly. This is especially true within the EU, where data protection regulations are already considered to be among the most stringent worldwide, as the new data protection regulation is expected to be passed into law in the near future (see text box "EU data protection regulation" over the page). This new regulation will apply not just to organisations in the EU, but also to any organisation that processes or stores information related to EU citizens. According to research conducted by Protiviti and ISACA, the lead taken by the EU is likely to be reflected in regulatory changes worldwide. African and Asian countries are moving towards the EU model, and those in Latin America either already have laws consistent with the EU model or are moving towards this. In the US, legislation and enforcement trends are for more privacy regulation, and federal-level data protection and privacy legislation is being considered.

Amendments to data protection laws will fundamentally change the way that organisations will have to deal with threat assessment and incident response. In practice, this will mean an obligation to maintain appropriate security controls, with a greater emphasis on the use of proactive monitoring technologies and the ability to detect and respond to security breaches faster and more efficiently.

## Use cases

The use of a SIEM system will go a long way in helping organisations to prove compliance with more draconian data protection and privacy regulations, as well as the other regulations and standards that they face, many of which are increasingly recommending the use of proactive, continuous monitoring controls to improve security. They also help with achieving compliance with security frameworks that organisations voluntarily choose to implement in order to manage risks, reduce the impact of security breaches, and provide assurance over their information security practices to business partners and customers.

The SANS Institute states that "By defining which events are of interest and what should be done about them, security and log analysis not only aids in compliance, but becomes proactive. Log analysis used in this manner can be used to detect emerging threats and trends, and even to tune and improve overall security." It states that, with regard to regulatory compliance, there are a few core elements to success that are provided by the use of SIEM systems:

- Log all relevant events
- Define the scope of coverage
- Define what events constitute a threat
- Detail what should be done about them in what time frame
- Document when they occurred and what was done
- Document where both the events and follow up records can be found
- Document how long events and tickets are kept

### EU data protection regulation

Current data protection laws in the EU have been enacted as a result of obligations under the data protection directive of 1995. Every member state has implemented the requirements of the directive into their own legislation, although each has been able to interpret the directive as it sees fit, as long as the basic requirements are met. This has resulted in a patchwork of laws across the EU, with laws varying from country to country.

The EU is looking to update this legislation in order to level the playing field across all member states, as well as to take into account recent developments in technology and electronic communications. One key change is that the new legislation will be a regulation, rather than a directive, which means that compliance is mandatory, without the need for national implementing legislation. Although no date has yet been finalised regarding when the regulation will become law, compliance looks set to become mandatory in 2016.

Among the key changes are increased fines and sanctions for non-compliance and the introduction of mandatory breach notification across all industry sectors. Fines of up to 5% of revenues or €100 million, whichever is greater, are being introduced for breaches suffered—and there is no minimum level regarding the size of the breach. All breaches will be subject to sanctions. Further, breaches must be notified within an extremely short notification window—currently slated to be within 24 hours of the breach occurring—which could prove to be disastrous for organisations that have not got their houses in order.

# The vendor

## Vendor background

SolarWinds was founded in 1999 and is a vendor of a broad range of IT management products aimed at helping organisations to manage their IT infrastructures, including fault and performance management, configuration management and compliance, and trouble-shooting applications across servers, databases, networks, applications, data storage and security systems.

Originally based in Oklahoma, SolarWinds relocated to Austin, Texas, in 2006, where it still maintains its headquarters. It has since expanded both within the US and internationally, with a number of offices in Europe and Asia, and is looking for further international expansion. In 2013, SolarWinds announced its intention to invest US$50 million in a new operations hub in Salt Lake City in Utah. It currently has more than 1,200 employees in 13 offices worldwide. SolarWinds has been a public company since its IPO in 2009.

SolarWinds has won a number of awards—both for its products and for its company performance. In 2012, Forbes recognised SolarWinds as the best small company in America, awarded to public companies with revenues under US$1 billion, with rankings based on return on equity, sales and earnings growth, and stock performance in relation to peers. Forbes called SolarWinds out for its high functioning products, low cost and impressive company growth. Also in 2012, it was included in the Deloitte Technology Top 500 for the sixth consecutive year. In terms of product awards, it has recently been recognised by Windows IT Pro, TechTarget and SC Magazine.

## Customers

SolarWinds claims to service some 100,000 customers worldwide, ranging from small companies to more than 425 of the Fortune 500 organisations. However, its primary target market is the mid-market as well as departments and branches of organisations. Many of its mid-market customers have small IT teams that are often over-stretched owing to the scarcity of resources.

## Competitors

The main competitors of SolarWinds LEM are large enterprise IT management vendors such as IBM and HP and security vendors such as McAfee and RSA. Other vendors that SolarWinds LEM compete with include Splunk and LogRhythm. SolarWinds' competitive position is a focus on core functionality and remediation capabilities at a very affordable price. In addition, it touts its superior out-of-the-box usability and speed of deployment as differentiators.

## Partners

SolarWinds works with a wide variety of partners, including a network of channel partners throughout the world to service local customers. It has a number of partnerships with hardware and software technology providers and with managed security service providers that offer hosted versions of its technology. Strategic partnerships include Microsoft and Cisco Systems.

## Financial information

SolarWinds is a public company having undergone an IPO in 2009 through which it raised US$112.5 million, and is listed on the New York stock exchange. In 2012, it achieved revenues of US$269 million, a growth of 36% over 2011, and operating margins of 53.8%. This sales growth is roughly in line with annual growth rates achieved in recent years. According to financial media firm, TheStreet, the growth rates achieved by SolarWinds are well above the current industry average of 6.4%.

## Summary

Security incidents and attacks leading to security breaches are growing both in volume and severity, making them increasingly hard to defend against. Every organisation should not only consider itself a target, but should assume that it has already been breached. A security stance based on preventing threats is no longer sufficient. Rather, organisations need to focus on developing robust capabilities for responding to incidents that have occurred. At the same time, government and industry mandates demanding high standards of security be maintained are increasing. In particular, data protection and privacy legislation is being expanded, affecting organisations of all sizes in all industries.

SolarWinds LEM provides for the needs of organisations of all sizes, but is particularly suited to those of mid-market organisations that often lack the budget and resources to implement and manage overly complex technology platforms. It is priced at a level that makes it easily affordable for such organisations, offering features comparable with SIEM systems aimed at large enterprises. Designed with usability in mind, specialised security expertise is not required to implement or manage the system, or to achieve the benefits of an improved overall security posture and greater ease of achieving compliance objectives that it provides.

### Further Information

Further information about this subject is available from
http://www.BloorResearch.com/update/2202

## Bloor Research overview

Bloor Research is one of Europe's leading IT research, analysis and consultancy organisations. We explain how to bring greater Agility to corporate IT systems through the effective governance, management and leverage of Information. We have built a reputation for 'telling the right story' with independent, intelligent, well-articulated communications content and publications on all aspects of the ICT industry. We believe the objective of telling the right story is to:

- Describe the technology in context to its business value and the other systems and processes it interacts with.
- Understand how new and innovative technologies fit in with existing ICT investments.
- Look at the whole market and explain all the solutions available and how they can be more effectively evaluated.
- Filter "noise" and make it easier to find the additional information or news that supports both investment and implementation.
- Ensure all our content is available through the most appropriate channel.

Founded in 1989, we have spent over two decades distributing research and analysis to IT user and vendor organisations throughout the world via online subscriptions, tailored research services, events and consultancy projects. We are committed to turning our knowledge into business value for you.

## About the author

**Fran Howarth**
Senior Analyst - Security

Fran Howarth specialises in the field of security, primarily information security, but with a keen interest in physical security and how the two are converging. Fran's other main areas of interest are new delivery models, such as cloud computing, information governance, web, network and application security, identity and access management, and encryption.

Fran focuses on the business needs for security technologies, looking at the benefits they gain from their use and how organisations can defend themselves against the threats that they face in an ever-changing landscape.

For more than 20 years, Fran has worked in an advisory capacity as an analyst, consultant and writer. She writes regularly for a number of publications, including Silicon, Computer Weekly, Computer Reseller News, IT-Analysis and Computing Magazine. Fran is also a regular contributor to Security Management Practices of the Faulkner Information Services division of InfoToday.

## Copyright & disclaimer

2nd Floor,
145–157 St John Street
LONDON,
EC1V 4PY, United Kingdom

Tel: +44 (0)207 043 9750
Fax: +44 (0)207 043 9748
Web: www.BloorResearch.com
email: info@BloorResearch.com